UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/014,873	12/14/2001	Jonathan Edwards	19903.0012	1763

23517   7590   09/16/2005

SWIDLER BERLIN LLP
3000 K STREET, NW
BOX IP
WASHINGTON, DC 20007

EXAMINER
ZAND, KAMBIZ

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Kambiz Zand

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *12/18/2002*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   **Claims 1-39** have been examined.

Information Disclosure Statement PTO-1449

.

2.   The Information Disclosure Statement submitted by applicant on 12/18/2002 has

been considered. Please see attached PTO-1449.

.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by
> another filed in the United States before the invention by the applicant for patent or (2) a patent
> granted on an application for patent by another filed in the United States before the invention by the
> applicant for patent, except that an international application filed under the treaty defined in section
> 351(a) shall have the effects for purposes of this subsection of an application filed in the United States
> only if the international application designated the United States and was published under Article 21(2)
> of such treaty in the English language.

.

4.   **Claims 1-39** are rejected under 35 U.S.C. 102(e) as being anticipated by Le

Pennec et al (2001/0020272 A1).

.

As per claims 1, 14 and 27 Le Pennec et al (2001/0020272 A1) teach a method,

system and computer program product of detecting a malware comprising the steps of:

monitoring file access operations of a process (see page 2);

intercepting a file access operation of the process to a file (see page 2, paragraph 0042

and 0043);

waiting a time interval (see page 2, paragraph 0046-0050); and

scanning the file for a malware (see page 2, paragraph 0046-0050).

As per claims 2, 15 and 28 Le Pennec et al (2001/0020272 A1) teach the method,

system and computer program product of claims 1, 14 and 27, wherein the process is

associated with an application program (see page 2-16 where many instances relates to

the above limitation).

As per claims 3, 16 and 29 Le Pennec et al (2001/0020272 A1) teach the method,

system and computer program product of claims 1, 14 and 27, wherein the file access

operation is a file write operation (see page 2-16 where many instances relates to the

above limitation).

As per claims 4, 17 and 30 Le Pennec et al (2001/0020272 A1) teach the method,

system and computer program product of claims 1, 14 and 27, wherein the file has a

specified file type (see page 2-16 where many instances relates to the above limitation).

.

As per claims 5, 18 and 31 Le Pennec et al (2001/0020272 A1) teach the method,

system and computer program product of claims 1, 14 and 27, wherein the time interval

is predefined (see page 2, paragraph 0046-0050).

As per claims 6, 19 and 32 Le Pennec et al (2001/0020272 A1) teach the method,

system and computer program product of claims 1, 14 and 27, wherein the time interval

is user-defined (see page 2 where setting the manual time interval is considered as user

defined time interval).

As per claims 7, 20 and 33 Le Pennec et al (2001/0020272 A1) teach the method,

system and computer program product of claims 1, 14 and 27, wherein the time interval

is based on a filetype of the file (see page 2-16 where many instances relates to the

above limitation).

As per claims 8, 21 and 34 Le Pennec et al (2001/0020272 A1) teach the method,

system and computer program product of claims 1, 14 and 27, wherein the time interval

is based on the process(see page 2-16 where many instances relates to the above

limitation).

As per claims 9, 22 and 35 Le Pennec et al (2001/0020272 A1) teach the method,

system and computer program product of claims 1, 14 and 27, wherein the malware is a

computer virus (see page 2).

As per claims 10, 23 and 36 Le Pennec et al (2001/0020272 A1) teach the method,

system and computer program product of claims 1, 14 and 27, wherein the malware is a

computer worm (see page 2-5).

As per claims 11, 24 and 37 Le Pennec et al (2001/0020272 A1) teach the method,

system and computer program product of claims 1, 14 and 27, wherein the malware is a

Trojan horse program.

As per claims 12, 25 and 38 Le Pennec et al (2001/0020272 A1) teach the method,

system and computer program product of claims 1, 14 and 27, further comprising the

step of: allowing the intercepted file access operation of the process to a file to complete

((see page 2-16 where many instances relates to the above limitation).

As per claims 12, 26 and 39 Le Pennec et al (2001/0020272 A1) teach the method,

system and computer program product of claims 12, 54 and 38, further comprising the

step of: allowing at least one additional file access operation of the process to a file that

occurs before the scanning of the file for a malware to complete (see page 2-16 where

many instances relates to the above limitation).

Conclusion

5.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure: see enclosed PTO-892.

6. Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Kambiz Zand whose telephone number is (571)

272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone

numbers for the organization where this application or proceeding is assigned as

(571) 273-8300. Information regarding the status of an application may be

obtained from the Patent Application Information Retrieval (PAIR) system. Status

information for published applications may be obtained from either Private PAIR

or Public PAIR. Status information for unpublished applications is available

through Private PAIR only. For more information about the PAIR system, see

http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197

(toll-free).

Kambiz Zand

08/29/2005

AU2132